ΝΑΝΟΗΛΕΚΤΡΟΝΙΚΗ & ΚΒΑΝΤΙΚΕΣ ΠΥΛΕΣ
4η Διάλεξη

Βιβλιογραφία: EXPLORATIONS IN QUANTUM COMPUTING, Colin P. Williams (2nd edition, Springer-Verlag, 2011), chapter 1.

Evolving a Quantum Memory Register

- Spectral Theorem for real symmetric matrices
- Schrödinger's Equation
- Hamiltonians
- Solution as a Unitary Evolution of the Initial State
- The no-cloning theorem
- Computational Interpretation

Spectral Theorem for real symmetric matrices

Let *A* be an *n* × *n* symmetric matrix with real entries. Then it has *n* real eigenvalues and one can choose an orthonormal eigenbasis $\{\mathbf{v}_1, \mathbf{v}_2, \ldots \mathbf{v}_n\}$. Using this basis to form the matrix: $V = \begin{bmatrix}\mathbf{v}_1 \, \mathbf{v}_2 \, \ldots \mathbf{v}_n\end{bmatrix}$, the matrix *A* is diagonalizable as: $A = VDV^t$, where the diagonal matrix *D* contains the eigenvalues in the diagonal:

$$D = \begin{pmatrix} \lambda_1 & 0 & 0 & \ldots & 0 \\ 0 & \lambda_2 & 0 & \ldots & 0 \\ 0 & 0 & \lambda_3 & \ldots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \ldots & \lambda_n \end{pmatrix}$$

For any vector **u**: $A\mathbf{u} = \sum_{i=1}^{n} \lambda_i (\mathbf{v}_i^t \cdot \mathbf{u})\mathbf{v}_i = \Big(\sum_{i=1}^{n} \lambda_i \mathbf{v}_i \mathbf{v}_i^t\Big)\mathbf{u}$ or $A = \sum_{i=1}^{n} \lambda_i \mathbf{v}_i \mathbf{v}_i^t$

Note that the matrix $\mathbf{v}_i \mathbf{v}_i^t$ is the orthogonal projection onto the vector $\mathbf{v}_i$ The action of a real symmetric matrix is that it projects the given vector into the eigendirections, scales the projected vectors by the corresponding eigenvalues, then adds up these scaled vectors.

MAKE SURE YOU TRULY UNDERSTAND IT. This is one of the most important tool whenever linear algebra is applied. In particular it enables us to define functions of matrices, such as e^{A}, sin(***A***) *etc*.

Spectral Theorem

Let A be a real symmetric $n \times n$ matrix and $f : \mathbf{R} \to \mathbf{R}$ a function. Then $f(A)$ is also an $n \times n$ matrix defined by its action on any vector $\mathbf{u}$ as

$$f(A)\mathbf{u} = A\mathbf{u} = \sum_{i=1}^{n} f(\lambda_i)(\mathbf{v}_i^t \cdot \mathbf{u})\mathbf{v}_i$$

In other words

$$f(A) = \sum_{i=1}^{n} f(\lambda_i)\mathbf{v}_i\mathbf{v}_i^t$$

if $A = VDV^t$ is the diagonalization of A, then : $f(A) = Vf(D)V^t$

where $f(D)$ for a diagonal matrix D is

$$f(D) = \begin{pmatrix} f(\lambda_1) & 0 & 0 & \dots & 0 \\ 0 & f(\lambda_2) & 0 & \dots & 0 \\ 0 & 0 & f(\lambda_3) & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & f(\lambda_n) \end{pmatrix}$$

For example: $A^2 = AA = \left(\sum_{i=1}^{n} \lambda_i \mathbf{v}_i \mathbf{v}_i^t\right)\left(\sum_{i=1}^{n} \lambda_i \mathbf{v}_i \mathbf{v}_i^t\right)$ with the function $f(x) = x^2$: $A^2 = \sum_{i=1}^{n} \lambda_i^2 \mathbf{v}_i \mathbf{v}_i^t$

For example $f(A)g(A) = (fg)(A)$, *then :* $\left(\sum_{i=1}^{n} f(\lambda_i)\mathbf{v}_i\mathbf{v}_i^t\right)\left(\sum_{i=1}^{n} g(\lambda_i)\mathbf{v}_i\mathbf{v}_i^t\right) = \sum_{i=1}^{n} f(\lambda_i)g(\lambda_i)\mathbf{v}_i\mathbf{v}_i^t$

Example on the spectral decomposition of a matrix

Find the spectral decomposition of the matrix $A = \begin{pmatrix} 2 & 2 & 1 \\ 2 & -1 & -2 \\ 1 & -2 & 2 \end{pmatrix}$

The characteristic polynomial is $p(\lambda) = det(\lambda - A) = \lambda^3 - 3\lambda^2 - 9\lambda + 27$

It easily factorizes: $\lambda^3 - 3\lambda^2 - 9\lambda + 27 = \lambda^2(\lambda - 3) - 9(\lambda - 3) = (\lambda + 3)(\lambda - 3)^2$

Hence $\lambda_1 = -3, \lambda_2 = \lambda_3 = 3$ i.e., the eigenvalue 3 has multiplicity 2.

First find the eigenvector $\mathbf{v}_1$ to $\lambda_1 = -3$ Then eigenvector $\mathbf{v}_1$ solves $A\mathbf{v}_1 = -3\mathbf{v}_1$, and $\mathbf{v}_1 = \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}$ The other eigenvalue is double Hence we need to find an orthonormal basis in the solution space $A\mathbf{v} = 3\mathbf{v}$. After row elimination on $A - 3I$ we get

$A - 3I = \begin{pmatrix} -1 & 2 & 1 \\ 2 & -4 & -2 \\ 1 & -2 & -1 \end{pmatrix} \Longrightarrow \begin{pmatrix} -1 & 2 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ and the nullspace of the matrix $A - 3I$

$N(A - 3I) = \left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix} \right\}$ The vectors $\mathbf{v}_2 = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \mathbf{v}_3 = \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}$ are linearly independent,

Example on the spectral decomposition of a matrix

hence the matrix of eigenvectors is $V = \begin{pmatrix} -1 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$ and $A = VDV^{-1}$ with

$D = \begin{pmatrix} -3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$ This is the diagonalization of A, but the eigenvectors are not orthonormal.

Recall that A is symmetric, and eigenvectors belonging to different eigenvalues are orthogonal.

Notice that $\mathbf{v}_1$ is really orthogonal to $\mathbf{v}_2, \mathbf{v}_3$. Although $\mathbf{v}_1$ is not normalized, it is easy to normalize it

$\mathbf{q}_1 = \frac{\mathbf{v}_1}{\|\mathbf{v}_1\|} = \frac{1}{\sqrt{6}} \begin{pmatrix} -1 \\ 2 \\ 1 \end{pmatrix}$ instead of $\mathbf{v}_1$ as eigenvector for λ_1. But $\mathbf{v}_2, \mathbf{v}_3$ are not orthogonal yet.

This is because we essentially chose an arbitrary (or most convenient) basis in $N(A - 3I)$.

So we have to run Gram-Schmidt for $\mathbf{v}_2, \mathbf{v}_3$: $\mathbf{q}_2 := \frac{\mathbf{v}_2}{\|\mathbf{v}_2\|} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$ and

$$\mathbf{w}_3 = \mathbf{v}_3 - (\mathbf{v}_3 \cdot \mathbf{q}_2)\mathbf{q}_2 = \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix} \quad \text{hence} \quad \mathbf{q}_3 = \frac{\mathbf{w}_3}{\|\mathbf{w}_3\|} = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ -1 \end{pmatrix}$$

Example on the spectral decomposition of a matrix

Now $\mathbf{q}_1, \mathbf{q}_2, \mathbf{q}_3$ is an orthonormal eigenbasis, and we can form the matrix

$$Q = \begin{pmatrix} -1/\sqrt{6} & 1/\sqrt{2} & 1/\sqrt{3} \\ 2/\sqrt{6} & 0 & 1/\sqrt{3} \\ 1/\sqrt{6} & 1/\sqrt{2} & -1/\sqrt{3} \end{pmatrix}$$

hence $A = QDQ^t$ (notice that the D matrix is the same, the eigenvalues did not change, only the eigenvectors), and this is the spectral decomposition of A.

Hence we learned how to find a basis in the nullspace of a matrix

first you have to find a basis in each nullspace $N(A - \lambda_j I)$

(which is the same as the eigenspace belonging to the eigenvalue λ_j),

then you have to orthonormalize this basis within each eigenspace

by the Gram-Schmidt procedure.

Evolving a Quantum Memory Register: Schrödinger's Equation

Our working assumption has been that the instantaneous state of a quantum memory register, $|\psi(t)\rangle$, holds the instantaneous state of the quantum computation.
But how does this state evolve with time, and how can we control this evolution in quantum computation?

Schrödinger's equation is a linear first order deterministic partial differential equation that involves the instantaneous state of the quantum memory register $|\psi(t)\rangle$:

$$i\hbar\frac{\partial|\psi(t)\rangle}{\partial t} = \mathcal{H}|\psi(t)\rangle$$

- $\mathcal{H}$ is a time independent Hermitian matrix, called ***the Hamiltonian*** (the observable for the total energy of the system),
- $\hbar$ is a constant equal to Planck's constant divided by 2π.

Normal operators ***A***: represent physical properties and their eigenvalues are the possible outcomes when the physical property is measured: $A^\dagger A = AA^\dagger$

A linear operator ***A*** is said to be

Hermitian if $A = A^\dagger$ and *Unitary* if $AA^\dagger = A^\dagger A = I$, the identity operator

All the details of a particular physical system are into the operator $\mathcal{H}$–the Hamiltonian.
So what does this Hamiltonian mean exactly?

Hamiltonians

- Quantum **observables** are described by operators, represented as Hermitian matrices.
- **Eigenvalues** are the allowed values for an observable of a Hermitian matrix.
- **Hamiltonian** is the observable corresponding to the total energy of the system, and its eigenvalues E_i are the possible values from measurements.
- $\mathcal{H}$ is a $2^n \times 2^n$ dimensional Hermitian matrix and there is always some basis (the energy eigenbasis $\{|\psi_i\rangle\}$) in which $\mathcal{H}$ is a diagonal matrix:

$$\mathcal{H} = \sum_i E_i |\psi_i\rangle\langle\psi_i| = \begin{pmatrix} E_0 & 0 & 0 & 0 \\ 0 & E_1 & 0 & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & E_{2^n-1} \end{pmatrix}$$

The solution of the Schrödinger equation

$$i\hbar \frac{\partial}{\partial t}\psi(t) = H\psi(t), \quad \psi(0) = \psi_0 \in \mathcal{H} \text{ (initial condition)},$$

can now be written as

$$\psi(t) = e^{-iHt/\hbar}\psi(0), \quad \text{provided that } H \text{ is independent of } t.$$

Then as $H = H^\dagger$: $e^{-iHt/\hbar}(e^{-iHt/\hbar})^\dagger = e^{-iHt/\hbar}e^{iH^+t/\hbar} = e^{-iHt/\hbar}e^{iHt/\hbar} = I,$

consequently, $e^{-iHt/\hbar}$ is unitary: $U(t) = \exp(-i\mathcal{H}t/\hbar)$

Solution as a Unitary Evolution of the Initial State

- As $\mathcal{H}$ is an Hermitian matrix, its matrix exponential $\exp(-i\mathcal{H}t/\hbar)$ is a unitary matrix.
- A unitary matrix has the property that its inverse is equal to its conjugate transpose: $U^{-1} = U^{\dagger}$.
- A unitary matrix is always invertible which means that the evolution it describes is reversible, i.e., there is no loss of information.
- Thus, the closest classical analog to quantum computing is classical ***reversible*** computing.

If the Hamiltonian is time-dependent: $H = H(t)$, then for an *infinitesimal* time step, from t to $t + dt$, we have

$$I - \frac{i}{\hbar} H(t) dt$$

for the unitary evolution operator. For continuous evolution with respect to time t, the solution of Schrödinger's equation cannot be represented in terms of a 1-parameter evolutionary group. Rather, a 2-parameter group *U(t, s)* is needed: ψ(t) = *U(t,0)*ψ(0),

where

$$\left.\begin{aligned} \frac{\partial}{\partial t} U(t,s) &= H(t) U(t,s) \\ \frac{\partial}{\partial s} U(t,s) &= -U(t,s) H(s) \end{aligned}\right\},$$

and *U(t, s')U(s', s) = U(t, s)*

U(t, s) remains unitary for any s, t.

Thus, *all quantum operations are unitary.*

Properties of Quantum Gates Arising from Unitarity

A matrix is unitary if: $U^{-1} = U^{\dagger}$. If U is unitary exhibits these properties:

- $U^{\dagger}$ is unitary.
- U^{-1} is unitary.
- $U^{-1} = U^{\dagger}$ (which is the criterion for determining unitarity).
- $U^{\dagger}U = \mathbb{1}$
- $|\det(U)| = 1$.
- The columns (rows) of U form an orthonormal set of vectors.
- For a fixed column, $\sum_{i=1}^{2^n} |U_{ij}|^2 = 1$.
- For a fixed row, $\sum_{j=1}^{2^n} |U_{ij}|^2 = 1$.
- $U = \exp(i\mathcal{H})$ where $\mathcal{H}$ is an hermitian matrix, i.e., $\mathcal{H} = \mathcal{H}^{\dagger}$.

for any quantum gate U.

1) $U^{\dagger}U = \mathbb{1}$ ensures that *a quantum gate is logically reversible*.

2) $\sum_{i=1}^{2^n} |U_{ij}|^2 = 1$ and $\sum_{j=1}^{2^n} |U_{ij}|^2 = 1$ ensure that if you start with a properly normalized quantum state and act upon it with a quantum gate, then you will end up with a properly normalized quantum state. *There are no probability "leaks".*

3) $|\det(U)| = 1$ means that the constraint on the determinant can be satisfied with $\det(U) = \pm 1$ or $\pm i$. *The elements of a general unitary matrix are generically allowed to be complex numbers.*

The no-cloning theorem

The restriction of time evolution to unitary operators means that certain kinds of evolution are *impossible*. One impossible task is *quantum cloning*.

Suppose we have a system in an unknown state $|\psi\rangle$, and we wish to *copy* it, i.e., to transform a second system starting in some standard state $|0\rangle$ into the same state $|\psi\rangle$. Is there a unitary $\hat{U}$ such that, for any state $|\psi\rangle$: $\hat{U}\left(|\psi\rangle \otimes |0\rangle\right) = |\psi\rangle \otimes |\psi\rangle$?

If this is true, then also for $|\phi\rangle \neq |\psi\rangle$ there is $\hat{U}\left(|\phi\rangle \otimes |0\rangle\right) = |\phi\rangle \otimes |\phi\rangle$.

Consider now a superposition state $|\chi\rangle = \alpha|\psi\rangle + \beta|\phi\rangle$. By linearity,

$$\begin{aligned}\hat{U}(|\chi\rangle \otimes |0\rangle) &= \hat{U}(\alpha|\psi\rangle + \beta|\phi\rangle) \otimes |0\rangle = \alpha|\psi\rangle \otimes |\psi\rangle + \beta|\phi\rangle \otimes |\phi\rangle \\ &\neq (\alpha|\psi\rangle + \beta|\phi\rangle) \otimes (\alpha|\psi\rangle + \beta|\phi\rangle),\end{aligned}$$

so $\hat{U}(|\chi\rangle \otimes |0\rangle) \neq |\chi\rangle \otimes |\chi\rangle$ is a contradiction. Therefore, no such $\hat{U}$ exists.

No-cloning theorem: quantum information, unlike classical information, *cannot be copied.*

1) *the state $|\psi\rangle$ of a system is not an observable*. Given a quantum system, there is no way to tell in what state $|\psi\rangle$ it was prepared.
2) If the state $|\psi\rangle$ is known, the state can be "copied" by preparing another system. But it is impossible to copy an *unknown* quantum state.
3) Many techniques of classical information theory (such as protecting information by making redundant copies, or having a *fanout* gate from a single bit) are impossible in quantum information theory.

Computational Interpretation

- A *classical computer* follows a LOAD-RUN-READ cycle: LOAD data into the machine, RUN a program using these data as input, and then READ out the result.
- A *quantum computer* follows a PREPARE-EVOLVE-MEASURE cycle: PREPARE a quantum state, EVOLVE it on the quantum computer, and MEASURE the result.

- In a classical computer you can only load one input at a time, in a quantum computer you can prepare exponentially many inputs in the same amount of time.
- A classical computer can only run a computation on one input, a quantum computer can evolve a superposition of computations on all inputs in the same time.
- A classical computer can only read one output, whereas a quantum computer can compute certain joint properties of all the answers to a particular computational problem in the time it takes a classical computer to find just one of the answers.
- This gives quantum computers the potential to be much faster than any classical computer, even a state-of-art supercomputer.